AccuTerm 7.1 Lite Release Notes

Release 7.1c (11-07-2014)

AccuTerm 7 Lite is designed to run on Windows XP SP2 and above. It will not run on Windows 2000 or any Windows 9x or ME versions. It is a 32 bit Windows application, and requires an Intel x86 (32 or 64 bit) architecture CPU. It is *not* compatible with ARM processors (Windows CE, Windows Mobile, Windows RT).

Upgrading from AccuTerm 7.1a to AccuTerm 7.1c

AccuTerm release 7.1c provides updates to Secure Shell (SSH) and adds a new connection method: SSL/Telnet. An incompatibility in Windows 8.1 cryptographic support required a change in AccuTerm's SSH crypto functions. SSH host key verification was also added in this release. See the highlighted sections below for details on the new SSH and SSL features.

Upgrading from AccuTerm 7 to AccuTerm 7.1

The main focus of AccuTerm 7.1 is to add support for Unicode AccuTerm terminal sessions (green-screen). Enhancements or changes which are new to AccuTerm 7.1 compared to AccuTerm 7 are denoted by shaded text.

AccuTerm 7.1 Lite should be installed in a separate directory from other versions of AccuTerm. AccuTerm 7.1 does not share any common components with prior versions of AccuTerm. The default installation directory is C:\Program Files\Atlite71. The application data directory is the same as for AccuTerm 7 Lite: C:\Users*username*\AppData\Roaming\Asent\atwin70. This is where the dialing directory and ssh key files are stored.

Upgrading from AccuTerm 2K2 Lite to AccuTerm 7.1 Lite

AccuTerm 7.1 Lite should be installed in a separate directory from previous versions of AccuTerm (97, 2000, 2K2). Unlike previous AccuTerm versions, AccuTerm 7.1 does not share any common components with prior versions of AccuTerm. The default installation directory is C:\Program Files\Atlite71. The application data directory has moved to C:\Users*username*\AppData\Roaming\Asent\atwin70. This is where the dialing directory and ssh key files are stored.

Differences between AccuTerm 7.1 Lite & Standard

AccuTerm 7.1 Lite is based on the "single document interface" standard. To open more than one session, you need to open multiple copies of AccuTerm 7 Lite.

AccuTerm 7.1 Lite supports the following features:

Accurate emulations for ADDS, Wyse and VTxxx terminals
Serial, Modem, Telnet, Secure Shell (v1 & v2) and SSL/Telnet connections
IPV6
Integrated 10,000 line scrollback buffer
Copy and Paste to clipboard
Screen print & Slave printer
Automatic scalable fonts
Screen size up to 240 columns by 240 rows by 25 pages
Unicode (UTF-8) host character set encoding
Can be installed on a portable device such as flash drive

The following features are supported by the Standard version of AccuTerm 7, but are not available in the Lite version:

File Transfer with Wizard
Data Capture
VBA Scripting
Multiple document interface for multiple sessions
Macro Recorder
Automation
Visual styles
Pre-defined themes including Modern & Classic Windows
Screen background picture (wallpaper)
Images
Sounds
Customizable menu / toolbar
Session tabs
Function key button bar
GUI designer
GUI runtime
wED editor
MultiValue server

ObjectBridge
Execute DOS/Windows command from host

New MSI-based Installer

The AccuTerm 7.1 Lite installer has been redesigned using Microsoft Installer (MSI). The MSI installation file is wrapped in a standard EXE installer which allows the selection of the desired installation type. The EXE installer then launches the MSI install (msiexec) with appropriate options. As with AccuTerm 7 Lite, three installation modes are supported: normal (all users), personal (install for current user only), and portable (run from removable device). The silent install options have been changed from /q or /s to /SILENT or /VERYSILENT. The format of the setup.ini file used to customize the installation process has been changed. Please see the user manual or online help for more information.

Product Activation

The product activation has been updated in AccuTerm 7. The product can now be activated at any time without requiring a re-install. In the **Help** menu, there is a new selection: **Enter Activation Code**.

The Activation form has a check box: **Send registration details to AccuSoft over the Internet**. We recommend checking this box to register your copy of AccuTerm when it is activated. This will aid us in helping you in the event that you lose your activation code or have other support issues.

New Features - Main Program

The menu, toolbar and status bar have been completely revamped.

The default font for new sessions is now **DejaVu Sans Mono**. This font has better hinting for small character sizes than the **AccuTerm Legacy** TrueType font, and has decent Unicode character set coverage. In prior versions of AccuTerm, the **AccuTerm** font consisted of hand-tuned bitmap fonts for smaller character sizes and TrueType fonts for larger sizes. Because Windows bitmap fonts do not support Unicode, the supplied **AccuTerm Legacy (bitmap)** font is limited to the Latin-1 (ISO 8859-1) character set. The supplied **AccuTerm Legacy** TrueType font may also be used, however due to poor hinting, rendering quality at small character sizes will suffer. The **AccuTerm Legacy** True Type font also appears to have thinner strokes at larger sizes. The new DejaVu font is recommended.

In AccuTerm 7, the Settings dialog box has been completely re-designed. The new interface uses a tree to select the category of setting to display in the main pane of the dialog. Using the tree interface has made the settings more logical.

AccuTerm 7 supports independent settings for screen printing and slave printing.

Network features in AccuTerm 7 have been improved. IPV6 is now supported, as is "Internationalized Domain Names" (punycode). Support for D3 Device Licensing has been added to telnet and SSH.

SSH has an additional authentication protocol: Keyboard Interactive. This protocol is similar to Password, but is host-driven. It is in common use on many Linux versions. The difference between Keyboard Interactive and Password authentication is that Keyboard Interactive supports password expiration and changing (if supported by the host). AccuTerm 7.1 SSH supports two additional encryption algorithms: Diffie-Hellman group 14 key exchange (previously, only group 1 was supported), and RSA signatures (previously only DSS signatures were supported, but some Cisco routers require the RSA signature algorithm). SSH now supports Putty format private key files, so you can import DSA and RSA private keys generated using Putty's puttygen.exe program.

AccuTerm 7.1c SSH supports "host key validation", which can be used to protect against "man in the middle" attacks.

Unicode Support

To use Unicode (UTF-8) as your host character set encoding, select "Unicode (UTF-8)" from the **Host Character Set Encoding** drop-down list in the Session Settings -> Terminal -> Font & Character Set page. Select a suitable font to support the language(s) you intend to use. Configure your host to use UTF-8 encoding.

Note: if you attempt to display characters that are not defined in the selected font, Windows "font linking" will attempt to use another suitable font for those characters. Sometimes the results are acceptable, but if the linked font does not produce suitable results, choose a font that includes all of the characters for the scripts you intend to display.

At this time, only left-to-right text is supported. We plan on adding bidirectional support for mixed left-to-right and right-to-left text in a future release.

SSH Enhancements

Host key verification

Verification of a server's host key when establishing an SSH connection is a security feature that is standard in many other SSH implementations, but has not previously been supported by AccuTerm. This release addresses this issue by adding some new settings in the SSH configuration panel to specify the level of verification desired. The choices are:

None: the host key is not verified and AccuTerm assumes that you are connected to the desired host. This is how all previous versions of AccuTerm have behaved.

Trust on first use: if the key has not been established (first time you connect to a particular host), AccuTerm assumes that you are connected to correct host and its key is saved in your session configuration. The key is verified on subsequent connections. If verification fails, the connection is aborted.

Confirm change: a dialog is displayed if a change in the host key for a particular session is detected. Confirmation is required to complete the connection. If the host is confirmed, the new key is saved in the session configuration, otherwise the connection is aborted.

Verify host key fingerprint: requires that the host key fingerprint be manually entered in the SSH settings. If the key verification fails, the connection is aborted. The fingerprint is the MD5 or SHA1 hash of the host key, in hex.

If your host is running OpenSSH, you can use the ssh-keygen command to display the host key fingerprint and copy/paste the fingerprint into the Key Fingerprint box in AccuTerm's SSH settings. The command to display the RSA host key fingerprint is:

```
ssh-keygen -lf /etc/ssh/ssh_host_rsa_key.pub
```

To display the DSA host key fingerprint, change "rsa" to "dsa" in the above command.

Note: the ssh-keygen command displays the MD5 hash of the host key. You can use this fingerprint for host key verification *unless you are running AccuTerm in FIPS-140 mode.* In FIPS-140 mode, the MD5 hash algorithm is not supported, and you will need to use the SHA1 hash instead. At this time we are unaware of any Linux command to display the SHA1 hash of the host key.

Default SSH2 cipher changed to AES 128 in CTR mode

The default cipher used for SSH2 connections was changed from Triple DES to AES 128 bit in CTR mode. Security experts have discovered a weakness in CBC mode ciphers, and now recommend using CTR mode instead. This may affect the cipher used for SSH2 connections, if you are using the default cipher.

SSL/Telnet Connection

A new connection method, SSL/Telnet has been added to this release. This connection method establishes a secure SSL/TLS connection between AccuTerm and the host, then initiates a Telnet session within the SSL connection (tunnel). This provides privacy and optionally, authentication of both client and server. This connection method is provided primarily for users who need to connect to UniVerse, UniData and other MultiValue platforms running on Windows. These platforms do not support Secure Shell (SSH). Both UniVerse and UniData have support for SSL/Telnet. Other MultiValue platforms may be able to use this connection method by using an SSL proxy, such as stunnel. Please consult your U2

documentation for server configuration instructions. Setting up the server for SSL is not a trivial task. At minimum, a self-signed X.509 Server certificate must be installed on the server for SSL/Telnet to function.

In addition to the advanced Telnet options, which are the same for SSL/Telnet and normal Telnet, SSL/Telnet has options for validating the server certificate, and for specifying an optional client certificate. Server certificate validation can be selected from a drop-down list:

None: any server certificate is assumed to be valid.

Minimal: the server certificate's name, role, expiration and root certificate authority are ignored. The certificate is rejected only if it has been revoked.

Self-signed – disregard host name: the server certificate's name, role and root Certificate Authority are ignored. The certificate is rejected if it is expired or revoked.

Self-signed – verify host name: the server certificate's role and root Certificate Authority are ignored. The certificate is rejected if the certificate Common Name does not match the host name specified in the "Host Name or IP Address" for the session configuration. It is also rejected if it is expired or revoked.

Strict: the server's certificate must be issued by a trusted Certificate Authority, and it must be valid for use as a Server certificate. It must not be expired or revoked, and the Common Name must match the host name specified in the session configuration (Host Name or IP Address field).

Custom: various requirements for certificate validation can be individually selected, in the event that the typical validation levels are not appropriate for a given host.

If the host requires client authentication, a client certificate can be selected from the drop-down box. The drop-down lists all client certificates installed on the user's computer, showing the Common Name, the issuing Certificate Authority, and the certificate expiration date. The client certificate is used to authenticate the client to the server while establishing the SSL connection. Normal login credentials (user ID and password) may still be required to initiate the Telnet session.

New Escape Sequences (AccuTerm Programming)

Some new private escape sequences added to AccuTerm 7:

ESC STX p *mode* CR - selects the printer mode:
- *mode* = 0 - turns off auto or transparent print
- *mode* = 1 - turns on auto print
- *mode* = 2 - turns on transparent print
- *mode* = X - turns off auto or transparent print and closes the print job immediately

ESC STX 2 - Enables mouse input in SystemBuilder compatibility mode; turns on mouse cursor. Transmits mouse location whenever a mouse button is pressed.

ESC STX jS , ID , col , row , width , height , page CR - Saves a copy of the specified screen block (text, colors and visual effects) and terminal state in memory and associates the block with the specified identifier (ID) which can be an arbitrary alpha-numeric string (may not contain commas). Any number of screen blocks can be saved. Col and row specify the upper-left corner of the block. If either is omitted or null, zero is assumed. Width and height specify the size of the block. If width or height is omitted or null, the screen width or height is used. Page optionally specifies the terminal page for the block, and if omitted or null, the current page is used.

ESC STX jR , ID , col , row , page CR - Restores the screen block associated with the specified identifier (ID) to the screen. Col and row specify the upper-left corner of the destination. If either is omitted or null, the original position of the saved block is assumed. Page optionally specifies the terminal page for the destination, and if omitted or null, the current page is used.

ESC STX jD , ID CR - Deletes the screen block associated with the specified identifier (ID) from memory.

ESC STX yj, *name* CR - Queries status of a stored screen block. Sends a 0 or 1, followed by a CR, indicating if a block of the specified name exists in AccuTerm's screen block memory.